Notice of Allowability	Application No.	Applicant(s)	
	10/803,167	NAZZAL, ROBERT N.	
	Examiner	Art Unit	
	CARL COLIN	2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *communications filed on 7/13/2009 and interview held on 11/19/2009*.

2. ☒ The allowed claim(s) is/are *8, 11-15, and 18-22*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *11/19/2009* .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Carl Colin/
Primary Examiner, Art Unit 2433

DETAILED ACTION

Response to Arguments

1. In communications filed on 7/13/2009, applicant amends claims 1-9, 11, 15, and 16; cancels claims 10 and 17. The following claims 1-9, 11-16, and 18-22 are presented for examination.

2. Applicant's arguments filed on 7/13/2009 have been fully considered and they are persuasive as amended and in the light of the Examiner's amendment. All previous objections and rejections have been withdrawn.

EXAMINER'S AMENDMENT

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Shun Yao on 11/19/2009.

The application has been amended as follows:

1-7. (Cancelled)

8. (Currently amended) A method for detection of a new service involving a host in a network, the method comprises:

retrieving a baseline list of port and/or service protocols used by a host being tracked, the baseline list listing service and/or port protocols used by that host over a baseline period that is of a longer duration than a current period;

retrieving a current list of service and/or port protocols for the current period used by the host being tracked;

determining whether there is a difference in the protocols, by finding a protocol that was in the current list but was not in the baseline list; and if there is a difference;

determining whether the host is providing or using the new service;

determining if the host is sending traffic using a protocol not in the current list;

identifying an alert rule corresponding to whether the host is providing or using the new service; and

issuing an alert based at least on the identified alert rule and whether the host is providing or using the new service.

9. (Cancelled)

11. (Currently amended) The method of ~~claim 9~~ claim 8 further comprising:

retrieving a value corresponding to an alert severity level set for violation of the rule.

15. (Currently amended) A computer program product residing on a computer readable medium for detection of new services in a network, the computer program product comprising instructions for causing a computer to:

retrieve a baseline list of port and/or service protocols used by a host being tracked, the baseline list listing service and/or port protocols used by that host over a baseline period that is of a longer duration that a current period;

aggregating communication information between every host pair;

retrieve a current list of service and/or port protocols for the current period used by the host being tracked;

determine whether there is a difference in the protocols, by identifying a protocol that was in a the current list but was not in the baseline list; and if there is a difference;

determine whether the host is providing or using the new service;

determining if the host is sending traffic using a protocol not in the current list;

identify an alert rule corresponding to whether the host is providing or using the new service; and

issue an alert based at least on the identified alert rule and whether the host is providing or using the new service.

16. (Cancelled)

Allowable Subject Matter

4. Claims 8, 11-15, and 18-22 are allowed.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARL COLIN whose telephone number is (571)272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Primary Examiner, Art Unit 2433
November 20, 2009